UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/723,418 | 11/27/2000 | Li-Jau Steven Yang | 24528.00900 | 6964 |

7590 11/26/2004

John W Carpenter
Crosby Heafey Roach & May
PO Box 7936
San Francisco, CA 94120-7936

| EXAMINER | |
|---|---|
| ARANI, TAGHI T | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

DATE MAILED: 11/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/723,418 | YANG ET AL. | |
| | Examiner | Art Unit | |
| | Taghi T. Arani, Ph.D. | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *27 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-8 and 11-21* is/are rejected.

7)☒ Claim(s) *5,9 and 10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/30/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

**Claims 1-21 are pending for examination**

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 6 and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 6 recites the limitation "said predetermined data" in lines 8, page 29. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 recites the limitation "said hash machine" in lines 20, page 29. There is insufficient antecedent basis for this limitation in the claim.

Claims 17-21 recite the limitation " The method according to Claim 1" in lines 10, 161, 5, and 6" respectively.

There is insufficient antecedent basis for this limitation in the claim. Claim 1 is An accelerator device (A system/apparatus claim). Claims 17-21 refers to a "method claim 1". Method claims cannot be depending from an apparatus base claim.

For purpose of applying art, the Examiner assumes "The method according to Claim 12".

### *Claim Rejections - 35 USC § 102*

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the

international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 4, 7, 11-12 and 14-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Krishna et al., U.S. Patent Application Publication No. 2003/0023846, published Jan. 2003.

**As per claim 1**, Krishna et al. teach an accelerator device, comprising:

an input buffer connected to a packet source and configured to accept and store packets from the packet source [Fig. 3, FIFO input unit (302), see also page 4, paragraph 0051];

a scanner configured to scan predetermined fields of the accepted/stored packets [Fig. 3, Packet classifier unit (304), page 4, paragraph 0051, i.e. packet header information is send to classification engine which determines security association information for processing the packet such as encryption keys, data etc.]; and

a modifier configured to modify fields of packets in said input buffer based on the scanned predetermined fields [ Crypto/Auth (316), see also page 4, paragraph 0052].

**As per claim 2**, Krishna et al. teach the accelerator according to Claim 1, wherein:

said predetermined fields are IPSEC fields of IP packets [page 5, paragraph 0058];and

said modifier comprises a processor configured to at least one of encrypt and decrypt IPSEC fields in said Packets [page 4, paragraph 0052, i.e. cryptographic processing unit for security processing. i.e. crypto engine including encryption/decryption].

**As per claim 4**, Krishna et al. teach the accelerator according to Claim 1, wherein said scanner scans the predetermined fields of the packets as they are being accepted/stored [page 3, paragraph 0038, i.e. from the input FIFO 202 packet header information (predetermined fields of the packets) is sent to a packet classifier 204].

**As per claim 7**, Krishna et al. teach the accelerator according to Claim 1, further comprising:

a hash state machine configured to generate an SA lookup index (SA ID) based on the predetermined scanned fields [page 6, paragraphs 0072, 0074 and 0078, i.e. a hash table structure to look up an entry in the security association table classification]

**As per claim 11**, Krishna et al. teach a hardware accelerator device, comprising: parser means connected to an input packet source for parsing predetermined fields of an inbound packet [Fig. 3, FIFO input unit (302), i.e. a packet source, Packet classifier unit (304), page 4, paragraph 0051, i.e. packet header information is send to classification engine which determines security association information for processing the packet such as encryption keys, data etc., see also page 4, paragraph 0051];

hash means for determining a security identification of the inbound packet [page 10, paragraph 0125, i.e. hash value based on destination address, spi and protocol, page 6, paragraph 0074, see also Fig. 6A element 604];

storage means for temporarily storing the parsed predetermined fields and said security identification [page 6, paragraph 0075, i.e. DRAM, see also page 10, paragraph 0125, for DRAM refill];

decryption means for deciphering encrypted data of the inbound packet based on programming [Fig. 61, element 610, see also page 7, paragraph 0091];

security database means for storing retrievable security associations [page 6, paragraph 0091, i.e. SAD, see also page 9, paragraphs 0112-0114]; and

Control/Data means (page 9, paragraph 0114, i.e. a control software to generate one non-overlapping match table entry for every combination that is active] for,

retrieving security associations from said database [page 9, paragraph 0116, i.e. security association table cache- Classification field (SATC-CL) used to look up a packet's classification fields on-chip, Fig. 6A, element 604),

programming the decryption mechanism based on at least one of the stored security information, other data contained in the incoming packet corresponding to the stored security information, and the retrieved security association [Fig. 6A, elements 610] , and

modifying fields of the incoming packet based on deciphered output of said decryption mechanism [Fig. 6A, elements 610, 612 and 614].

**As per claim 12**, Krishna et al. teach a method of performing IPSEC processing,

comprising: scanning a packet for IPSEC related information [Fig. 3, Packet classifier unit (304), page 4, paragraph 0051, i.e. packet header information is send to classification engine which determines security association information (IPSEC related information) for processing the packet such as encryption keys, data etc.];

programming an IPSEC services device to perform IPSEC processing based on the scanned IPSEC information [ Crypto/Auth (316), see also page 4, paragraph 0052]; and

providing data from said packet for processing by the IPSEC services device (packet header information is send [pag4 4, paragraph 051, i.e. provided) to classification

engine which determines security association information, see also page 5, paragraph 063]; and

modifying said packet based on an output from the IPSEC security services device {Fig. 6, elements 668];

wherein said steps of scanning, programming, providing, and modifying are performed by a hardware device at an IP layer of a network connected device [page 2, paragraph 0027-028, i.e. the cryptography acceleration chip is part of standard network line card (i.e. a hard ware device at an IP layer of a network (LAN or WAN interface) and manages (i.e. scanning, programming, providing and modifying) in-bound and out-bound IP packets, see also page 3, paragraph 0033 and paragraph 0037].

**As per claim 14**, Krishna et al. teach the method according to Claim 12, wherein said IPSEC related information comprises data contained in at least one of Authentication (AH), and Encapsulating Security Payload (ESP) fields of said packet [page 9, paragraph 0106].

**As per claim 15**, Krishna et al. teach the method according to Claim 12, wherein said step of programming includes the steps of,

determining a security association by indexing a security association database [page 6, paragraph 074 and 078] with at least part of the scanned IPSEC related information [such as spi and protocol, etc.] and providing the determined security association to the IPSEC services device [page 3, paragraph 0039, i.e. the distributor unit determines and distributes the security association information SA received from the packet classification unit among a plurality of cryptography processing engines].

**As per claim 16**, Krishna et al. teach the method according to Claim 12, further comprising the steps of:

hashing at least one field of said packet to determine a security association ID (SA ID) [page 6, paragraph 0074];

determining a security association by looking up a security association in an SA database based on the SA ID [page 7, paragraph 092. i.e. parsing the header and a security association lookup is conducted]; and

utilizing the security association as part of the programming provided to the security services device [page 7, paragraph 0092 i.e. the packet is encapsulated, encrypted and authenticated utilizing security association].

**As per claim 17**, Krishna et al. teach the method according to Claim 1 [12], wherein:

said step of scanning comprises scanning said packet as it is being received from a packet source [page 3, paragraph 0038, i.e. from the input FIFO 202 packet header information (predetermined fields of the packets) is sent to a packet classifier 204]; and

said packet source is one of a network card and upper layers of a host protocol stack [ page 2, paragraphs 0028-029].

**As per claim 18**, Krishna et al. teach the method according to Claim 1 [12], wherein said step of providing comprises the steps of:

reading at least part of said packet from a buffer device storing said packet [page 3, paragraph 0037, i.e. FIFO feeds classification information along with packet data]; and

providing at least part of the data read as input to said IPSEC security services device [page 3, paragraph 038, from input FIFO 202, the header information is sent to packet classifier unit 204].

**As per claim 19**, Krishna et al. teach the method according to Claim 1[12], wherein said steps of scanning, programming, providing, and modifying are performed within the IP layer of the network protocol stack [page 2, paragraph 0027-028, i.e. the cryptography acceleration chip is part of standard network line card (i.e. a hard ware device at an IP layer of a network (LAN or WAN interface) and manages (i.e. scanning, programming, providing and modifying) in-bound and out-bound IP packets, see also page 3, paragraph 0033 and paragraph 0037] .

**As per claim 20**, Krishna et al. teach the method according to Claim 1[12], wherein said step of

modifying comprises:

when said packet is using Encapsulating Security Payload and said packet is in transport mode [see Fig 7 for features recited],

adding ESP, ESP Trailer, and ESP Auth fields to said packet [page 9, paragraph 0106 ],

encrypting the ESP, TCP, Data, and ESP Trailer fields, and

authenticating the ESP, TCP, Data, and ESP Trailer fields [page 10, paragraph 0121, see also page 9, paragraphs 0106-01116] ;

when said packet is using Encapsulating Security Payload

and when said packet is in tunnel mode [page 9, paragraph 0106],

adding a new IP header, ESP, ESP Trailer, and ESP Auth fields to said packet

[page 9, paragraph 0107 and 0116],

encrypting the original IP header, TCP, Data, and ESP Trailer fields of said packet [Fig. 6B, elements 666 9encapsulate packet (new header) and 668 (perform encryption and authentication)], and

authenticating the ESP, original IP header, TCP, Data, and ESP Trailer fields of said packet [Fig. 6A elements 610 – 612, see also page 7, paragraph 0091, page 9, paragraph 0101];

when said packet is using Authentication Header and said packet is in transport mode [page 9, paragraph 0116, field name ipsec format (ESP, AH or none, Tunnel or Adj],

adding an AH field, and authenticating the entire packet except for mutable fields [page 9, paragraph 0107]; and

when said packet is using Authentication Header and said packet is in tunnel mode,

adding a new IP Header and AH field, and authenticating the entire packet except for mutable fields[page 9, paragraph 0116, field name peer@ (IP header), field name ipsec format (ESP, AH or none, Tunnel or Adj (transport)].

**As per claim 21**, Krishna et al. teach the method according to Claim 1[12], wherein said step of modifying comprises writing at least portions of said packet that are being added and/or modified by the security services device to a buffer storing said packet prior to shipment of said packet to one of a transport device or upper layer protocols of a host device [page 4, paragraph 0047, i.e. once the engine completes processing the packet, the processed packet is placed in a retirement buffer, the

retirement unit then extracts processed packets out of retirement buffer in the same order that the chip originally received the packets, and outputs processed packets ].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishna et el. as applied to claims 1 and 12 above, and further in view of below.

**As per claims 3 and 13**, the Examiner asserts that Mongoose type processor is well known in the art and it would have been an obvious matter of design choice to be employed in cryptographic processor of Krishna et al. for its on-chip caches which provides high bandwidth memory access to keep the CPU operating.

**As per claim 8**, The Examiner asserts that the polynomial hashing code is old and well known in the art. It would have been obvious to one of ordinary skill in the art to adapt Krishna et al.'s hash table to a Polynomial CRC to reduce possible large number of collisions in addressing memory locations.

***Allowable Subject Matter***

Claims 5, 9 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Prior arts made of record, not relied upon:

US 6,275,588 is directed to technique for performing compression, encryption and transmission, and reception, decryption and decompression, respectively, of data communication packages on an area network.

US 6,327,625 is directed to a FIFO-based network interface supporting out-of-order processing.

US 2001/047487 is directed to a network device implementing IPSec comprising at least one IP forwarder arranged to receive IP packets each of which is associated with a security association (SA).

US 2002/0062344 and US 6, 438,612 discuss security association for processing IP packets communicated between a transmitting virtual router and a receiving virtual router.

Child-proof Authentication for MIPv6 by Michael Rose et al. of Microsoft Research Ltd, discusses a specialized security system for Unilateral authentication in Mobile Ipv6 for use in the absence of comprehensive IPSEC implementation.

Mongoose-v 32-bit MIPS Microprocessor is an overview of the Mongoose processor.

RFC 2401 specifies an Internet Standards track protocol for the Internet Community relating to the base structure for IPsec compliant systems.

**Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (703)305-4274. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

***

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100